National Security Agency/Central Security Service

INFORMATION
ASSURANCE
DIRECTORATE

CGS Network Access Control Capability

Version 1.1.1

Network Access Control is the capability of the system/network to ensure that each endpoint meets security policies when it connects to the network. The intent of Network Access Control is to provide technical controls to ensure that only authorized computing platforms gain access to network resources.

07/30/2012

CGS Network Access Control Capability

Version 1.1.1

Table of Contents

1 Revisions

Name	Date	Reason	Version
CGS Team	30 June 2011	Initial release	1.1
CGS Team	30 July 2012	Inclusion of new IAD document template & Synopsis	1.1.1

2 Capability Definition

The Capability definition provides an understanding of the importance of the Capability to the Enterprise. It provides a high-level overview of the Capability based on definitions derived from Committee on National Security Systems (CNSS) Instruction No. 4009.

Network Access Control is the capability of the system/network to ensure that each endpoint meets security policies when it connects to the network. The intent of Network Access Control is to provide technical controls to ensure that only authorized computing platforms gain access to network resources. The Network Access Control capability can perform the following:

- Platform Authentication–Verifies the identity of a platform requesting access to a network
- Access Policy Compliance–Determines that a platform requesting network access complies with policy for such access
- Endpoint Policy Compliance–Establishes an endpoint‘s compliance with applicable configuration, patching, and approved software policy
- Assessment, Isolation, and Remediation–Isolates platforms not meeting requirements for access from the network and provides for configuration remediation to bring a platform into compliance

3 Capability Gold Standard Guidance

The Capability Gold Standard Guidance evaluates the Enterprise needs and overlays the expected Gold Standard behavior. The guidance goes beyond the concept of “good enough” when describing the Gold Standard recommendations, considers industry best practices, and describes a level of security that not only meets current standards but also exceeds them across the Enterprise.

The Network Access Control Capability provides a set of policies and procedures that are used to manage access to a network and all of its associated systems or resources. The Network Access Control Capability includes both connections coming into the Enterprise from external networks and connections traversing enclave boundaries internal to the Enterprise. Network Access Control applies to whatever is within the logical boundary, which may not be the same as the physical boundary (see Network Boundary and Interfaces Capability). All communications within this Capability shall be protected as necessary by the Communication Protection Capability.

Network Access Control shall perform the following functions:

Platform Authentication
Only limited, rudimentary network access shall be available for platforms prior to authentication. Platforms cover all devices with network connectivity including workstations, communications devices, routers, switches, and firewalls. This function prevents unauthorized attempts to physically connect to the network either through a wired or wireless connection. This function also prevents the attachment of rogue access points to the network. Platform Authentication shall verify the identity of the machine, user, and the attributes that are relevant such as the type of device, device owner, device location (including wired or wireless), and other attributes that are determined by the Enterprise. During Platform Authentication, reauthentication of the identity shall occur, as needed, to detect changes in the identity and ensure the system does not change during communications or idle system time. This reauthentication mechanism shall be robust enough to detect errors and prevent service disconnects from authorized platforms.

There shall be a level of assurance that the attributes are correct and not spoofed (come from a non-authoritative trusted source, as defined in Attribute Management and Identity Management). Internet Protocol (IP) and Media Access Control (MAC) address authentication can be spoofed and therefore shall not be used as the only means for authentication. Hardware modules (e.g., Trusted Platform Module [TPM]) shall be used on the connecting device for storage of the authentication attributes and shall be cryptographically protected. Cryptographic modules shall be compliant with any applicable federal and Community standards.

Access Policy Compliance
Access Policy Compliance shall use attributes that have been authenticated to make an access decision before providing network services. Access policy is defined in the Access Management Capability and enforced in Network Access Control. To enforce policy, there shall be an enforcement point at network boundaries that can effectively block access to resources in accordance with the defined access policy. As mentioned above, IP and MAC addresses can be spoofed and shall not be used alone. The association between the attributes and the identity shall be ensured, such as by using cryptographic binding, thus making the identity and attributes suitable for use by the enforcement point to make the access decisions.

Endpoint Policy Compliance

Endpoint Policy Compliance shall ensure (as provided by Configuration Management) the following:

- Presence, status, and software version of mandated applications (including the operating system [OS])
- Completeness of virus signature databases
- Completeness of intrusion detection and prevention system applications
- The acceptable patch level of all software

The Network Access Control Capability applies to endpoints running virtualization software and extends to the guest OS as well as the system running the virtualization software. The verification against Configuration Management baselines is provided in the Configuration Management repository (see the Configuration Management Capability). The Capability shall check for OS type, OS version, and OS updates.

Assessment, Isolation, and Remediation

Assessment measures the integrity of the endpoint, meaning it evaluates the purity of the endpoints from a software and hardware perspective. Analysis shall include malware and vulnerability detection based on policy and compliance checking. The assessment process shall include information gathered from the endpoint and observable behavior gathered from the Network Enterprise Monitoring Capability and other Detect Events Capabilities to perform the assessment. To enable assessment, endpoints shall support the Platform Trust Services Interface Specification that supports the collection of endpoint integrity status and detection of unauthorized modification. The endpoint shall store integrity information in the protected hardware module.

The endpoint shall be isolated until completion of the assessment. When the assessment is complete, the endpoint shall be granted full access, limited access, or remain isolated based on the assessment, as defined below:

- Full Access–Access is granted to all resources as defined in the Access Management, Attribute Management, and Digital Policy Management Capabilities. Risk to Enterprise assets is known and accepted when full access is provided.
- Limited Access–The assessment has determined that there is an issue, or limited access is based on the attributes (e.g., the platform is identified as a guest). In this case, the requester may not be approved for full access. Based on mission need, access is granted to limited resources as needed to carry out a mission.

Risk to Enterprise assets is known and accepted when this limited access is provided.

- Isolation–The endpoint is confined to a defined set of resources that is responsible for remediating the issues found during assessment. The amount of remediation applied shall be based on policy or attributes and may implement changes that will allow an endpoint only limited access. Full remediation may not be possible. In some cases, the endpoint may remain isolated or be denied access.

Isolation, limited access, remediation, and operational networks shall exist to allow for secure segregation. Protection mechanisms established by the Network Boundary Protection Capability shall be in place to enforce separation. Within the isolation and remediation networks, endpoints shall not be allowed to communicate with one another. During remediation, actions are taken to ascertain what the issues are with the endpoint’s integrity and necessary steps are taken to alleviate those issues. After remediation, the endpoint shall be reassessed prior to being granted access.

All of the actions of the Network Access Control Capability, including policy changes, shall be audited and provided to the Enterprise Audit Management Capability. The endpoint shall provide the results of the assessment (e.g., configuration status) to administrators. Depending on the endpoint connection, notification shall be sent to the Monitoring Capabilities for correlation of events or trend analysis. The Network Access Control Capability shall provide notification of successful and unsuccessful connection attempts, along with the reason for an unsuccessful attempt.

4 Environment Pre-Conditions

The environment pre-conditions provide insight into environmental, user, and technological aspects needed for Capability implementation. These pre-conditions are services or other Capabilities that must be in place within the Enterprise for the Capability to function.

1. Policy is defined for establishing connections to/from devices.
2. The access control policies are defined.
3. The network boundaries are known and documented.
4. The infrastructure can support remediation actions.
5. Configuration baselines are defined.

5 Capability Post-Conditions

The Capability post-conditions define what the Capability will provide. They define functions that the Capability will perform or constraints that the Capability will operate under when performing its function.

1. The Capability provides a proactive assessment of endpoint health and authentication information.
2. The Capability ensures Configuration Management policy is being followed.
3. All devices requesting access to a network will be authenticated prior to being granted access.
4. The Capability limits malware entry into the Enterprise.
5. The Capability applies to endpoints running virtualization software and extend to the guest OS.

6 Organizational Implementation Considerations

Organizational implementation considerations provide insight into what the Organization needs to establish, ensure, and have in place for the specified Capability to be effective. It provides guidance specific to the actions, people, processes, and departments that an Organization will need to execute or establish to implement the guidance described in Section 3 (Capability Gold Standard Guidance).

Network Access Control enforces the set of policies and procedures used to manage access to a network and all of its associated systems. Access comes from two places, physical connections from within the network and connections from an outside network.

Each Organization will perform platform authentication, access policy, endpoint compliance and assessment, isolation, and remediation for both connections coming into the Enterprise from external networks and connections traversing enclave boundaries internal to the Enterprise.

The Organization will provide protection devices to be used as enforcement points at each Network Boundary to block access to resources in accordance with the defined policy for Access Management.

When Network Access Control mechanisms detect a new device on the network that requires access, the endpoint will be forced to authenticate to the network. Each Organization will provide identities through the Identity Management Capability for use in this process. If the Identity is not provided by the Organization that owns the network, mechanisms will be in place to determine the identity. Relevant attributes (e.g., type of device, device owner, device location [including wired or wireless]) will be provided by an authoritative source published by the Attribute Management Capability. Machine-level authentication will be performed prior to access being granted based on the verification of identity and attributes. In some instances, Organizations may want to combine identification of the machine and user based on mobility requirements (e.g., wireless devices). The Organization will monitor connections to ensure identities are reauthenticated periodically based on mission drivers as defined by the Organization's policy.

The Organization will ensure that access control policies are defined for enforcement by Network Access Control. Access Management will then be invoked to determine access. Often, an authentication service such as Remote Authentication Dial-in User Service (RADIUS) is part of this function. Access policy uses the attributes that have been authenticated to make an access decision and provide network services.

The endpoint policy will be assessed for compliance as determined by the Organization's Configuration Management Capability. Once the assessment result is provided to the enforcement point, endpoint policy compliance will ensure the presence, status, and software version of mandated applications (including the OS); completeness of virus signature databases; intrusion detection and prevention system applications; and the acceptable patch level of all software (as provided by Configuration Management).

The Network Access Control Capability will grant access based on the assessment result. The assessment will measure the integrity of the endpoint. Each Organization will perform analysis, including malware and vulnerability detection, based on policy defined by the Organization. The assessment will include information gathered from the endpoint and observable behavior to understand what the endpoint does once it connects to the network. The Network Access Control Capability will use the Network Enterprise Monitoring Capability and other Detect Events Capabilities to gather the observable behavior information.

Isolation will start when the authentication process begins and will be enforced until completion of the assessment. The Organization will define the policy and actions for remediation based on mission needs and risk. Based on the assessment, the endpoint will be granted full access, limited access, or remain isolated. Access will be granted to a small set of resources that are needed based on mission requirements. This limited

access will remain until the problems found are resolved (e.g., latest virus definitions or system patches). Each Organization will define policy to determine how much remediation is applied based on attributes. After remediation, the Organization will perform another assessment to ensure problems are fixed prior to granting access. This cyclical process will continue until all problems are resolved.
Anytime a device is moved from isolation, the Organization will accept the risk to Enterprise assets. In some cases, a device may remain isolated. Each Organization will ensure appropriate network boundaries are in place to securely segregate isolation, limited access, remediation, and operational networks. Within all isolation networks, endpoints will not be allowed to talk to each other.

Organizations will leverage the Enterprise Audit Management Capability to ensure actions are audited for network access requests and policy changes (e.g., policy override by an administrator). Depending on the situation, an alert may be sent to Network Operations. Network Access Control will provide to the Organization insight on endpoint compliance and assessment results including successful and unsuccessful events with details. Each Organization will provide reports to Network Enterprise Monitoring for event correlation and trend analysis.

7 Capability Interrelationships

Capability interrelationships identify other Capabilities within the Community Gold Standard framework that the Capability in this document relies on to operate. Although there are many relationships between the Capabilities, the focus is on the primary relationships in which the Capabilities directly communicate with or influence one another.

7.1 Required Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are necessary for the Capability in this document to operate.

- Configuration Management–The Network Access Control Capability relies on the Configuration Management Capability to provide information on the configuration of policy decision devices and verification against the Configuration Management baseline.
- Network Boundary Protection–The Network Access Control Capability relies on the Network Boundary Protection Capability to enforce access decisions made at enforcement points on network boundaries.

- Identity Management–The Network Access Control Capability relies on information provided by the Identity Management Capability to ensure that only resources with known and approved identities are allowed access to the network.
- Digital Policy Management–The Network Access Control Capability relies on the Digital Policy Management Capability to manage and define the applicable digital policies.
- Attribute Management–The Network Access Control Capability relies on the Attribute Management Capability to assign attributes to entities and resources that are used for access control decisions.

7.2 Core Interrelationships

The following Capability interrelationships include the Capabilities within the Community Gold Standard framework that relate to every Capability.

- Portfolio Management–The Network Access Control Capability relies on the Portfolio Management Capability to determine current and future investment needs and prioritize investments based on those needs.
- IA Policies, Procedures, and Standards–The Network Access Control Capability relies on the IA Policies, Procedures, and Standards Capability to provide information about applicable federal laws, Executive Orders, regulations, directives, policies, procedures, and standards.
- IA Awareness–The Network Access Control Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.
- IA Training–The Network Access Control Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.
- Organizations and Authorities–The Network Access Control Capability relies on the Organizations and Authorities Capability to establish the relevant roles and responsibilities.

7.3 Supporting Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are not necessary for the Capability to operate, although they support the operation of the Capability in this document.

- Communication Protection–The Network Access Control Capability relies on the Communication Protection Capability to protect all of the communications that occur as a part of endpoint compliance activities.

- Network Enterprise Monitoring–The Network Access Control Capability relies on the Network Enterprise Monitoring Capability for information used to perform assessments of endpoint integrity.
- Risk Mitigation–The Network Access Control Capability implements countermeasures that may be selected by the Risk Mitigation Capability.

8 Security Controls

This section provides a mapping of the Capability to the appropriate controls. The controls and their enhancements are granularly mapped according to their applicability. In some instances, a control may map to multiple Capabilities.

Control Number/Title	**Related Text**
NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*	
AC-4 *INFORMATION FLOW ENFORCEMENT*	Control: The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy. Enhancement/s: (16) The information system enforces security policies regarding information on interconnected systems.
AC-17 *REMOTE ACCESS*	Control: The organization: a. Documents allowed methods of remote access to the information system; b. Establishes usage restrictions and implementation guidance for each allowed remote access method; c. Monitors for unauthorized remote access to the information system; d. Authorizes remote access to the information system prior to connection; and e. Enforces requirements for remote connections to the information system. Enhancement/s: (1) The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods. (3) The information system routes all remote accesses through a limited number of managed access control points.

	(4) The organization authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and documents the rationale for such access in the security plan for the information system. (6) The organization ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.
AC-18 *WIRELESS ACCESS*	Control: The organization: a. Establishes usage restrictions and implementation guidance for wireless access; b. Monitors for unauthorized wireless access to the information system; c. Authorizes wireless access to the information system prior to connection; and d. Enforces requirements for wireless connections to the information system. Enhancement/s: (1) The information system protects wireless access to the system using authentication and encryption. (2) The organization monitors for unauthorized wireless connections to the information system, including scanning for unauthorized wireless access points [Assignment: organization-defined frequency], and takes appropriate action if an unauthorized connection is discovered. (3) The organization disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment. (4) The organization does not allow users to independently configure wireless networking capabilities. (5) The organization confines wireless communications to organization-controlled boundaries.
CA-3 *INFORMATION SYSTEM CONNECTIONS*	Control: The organization: a. Authorizes connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements; b. Documents, for each connection, the interface

	characteristics, security requirements, and the nature of the information communicated; and c. Monitors the information system connections on an ongoing basis verifying enforcement of security requirements. Enhancement/s: (1) The organization prohibits the direct connection of an unclassified, national security system to an external network. (2) The organization prohibits the direct connection of a classified, national security system to an external network.
CM-8 *INFORMATION SYSTEM COMPONENT INVENTORY*	Control: The organization develops, documents, and maintains an inventory of information system components that: a. Accurately reflects the current information system; b. Is consistent with the authorization boundary of the information system; c. Is at the level of granularity deemed necessary for tracking and reporting; d. Includes [Assignment: organization-defined information deemed necessary to achieve effective property accountability]; and e. Is available for review and audit by designated organizational officials. Enhancement/s: (3) The organization: (a) Employs automated mechanisms [Assignment: organization-defined frequency] to detect the addition of unauthorized components/devices into the information system; and (b) Disables network access by such components/devices or notifies designated organizational officials.
SC-10 *NETWORK DISCONNECT*	Control: The information system terminates the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity. Enhancement/s: None Specified
SI-4 *INFORMATION SYSTEM MONITORING*	Control: The organization: a. Monitors events on the information system in accordance with [Assignment: organization-defined monitoring objectives] and detects information system attacks;

	b. Identifies unauthorized use of the information system; c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization; (14) The organization employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.

9 Directives, Policies, and Standards

This section identifies existing federal laws, Executive Orders, regulations, directives, policies, and standards applicable to the Capability but does not include those that are agency specific.

Network Access Control Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	
NSPD-54/HSPD-23 Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified	Summary: National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23), in which the Comprehensive National Cybersecurity Initiative (CNCI) is described, is classified. Initiative 7 deals with increasing the security of classified networks.
Department of Defense (DoD)	
DISA Network Infrastructure Security Technical Implementation Guide (STIG), version 7.1, 25 October 2007, Unclassified	Summary: This Security Technical Implementation Guide (STIG) provides security considerations at the network level needed to achieve an acceptable level of risk for information as it is transmitted through an enclave. It was developed to enhance the confidentiality, integrity, and availability of sensitive Department of Defense (DoD) Automated Information Systems.

DISA Secure Remote Computing Security Technical Implementation Guide (STIG), version 1.1, 2 October 2009, Unclassified	Summary: This STIG provides guidance for secure configuration and usage of devices used for remotely accessing DoD networks and to assist sites in meeting the minimum requirements, standards, controls, and options for secure remote computing. The guidance presented is specific to remote computing environments, above and beyond what is currently required by other DoD STIGs and applicable DoD policy.
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, …)	
Nothing found	
Executive Branch (EO, PD, NSD, HSPD, …)	
Nothing found	
Legislative	
Nothing found	

Network Access Control Standards

Title, Date, Status	**Excerpt / Summary**
Intelligence Community (IC)	
ICS 503-1, Interconnection Security Agreements, 28 January 2009, Unclassified	Summary: This standard identifies the standard for interconnection security agreements, which document, formalize, and stipulate specific requirements for Organizations that own and operate connected information technology systems.
Comprehensive National Cybersecurity Initiative (CNCI)	
Nothing found	
Department of Defense (DoD)	
Nothing found	

Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, …)	
FIPS 140-2, Security Requirements for Cryptographic Modules, 3 December 2002, Unclassified	Summary: This standard specifies the security requirements that will be satisfied by a cryptographic module used within a security system protecting sensitive but unclassified information.
Executive Branch (EO, PD, NSD, HSPD, …)	
Nothing found	
Legislative	
Nothing found	
Other Standards Bodies (ISO, ANSI, IEEE, …)	
IEEE Std 802.1X, Port-Based Network Access Control, raft version 2.1, 28 February 2008, Unclassified	Summary: This standard specifies a common architecture, functional elements, and protocols that support mutual authentication between the clients of ports attached to the same local area network (LAN).
Federated Trusted Network Connect (TNC), version 1.0, revision 26, May 2009, Unclassified	Summary: Trusted Network Connection (TNC) is an architecture consisting of a set of specifications designed to assist network administrators in protecting networks by allowing them to audit endpoint configurations and impose Enterprise security policies before network connectivity is established. It is an open, nonproprietary standard that enables the application and enforcement of security requirements for endpoints connecting to the corporate network. The specifications offer critical elements of Network Access Control that can be used now to create products to protect the network.
Trusted Network Connect (TNC) Architecture for Interoperability	Summary: This specification defines the TNC architecture for interoperable Network Access Control and authorization. It defines and promotes an open solution

Specification, version 1.4, revision 4, 18 May 2009, Unclassified	architecture that enables network operators to enforce policies regarding the security state of endpoints to determine whether to grant access to a requested network infrastructure.
Platform Trust Services Interface Specification, version 1.0, 17 November 2006, Unclassified	Summary: This specification defines architecture and specifications to enable enforcement of endpoint integrity when granting access to a network infrastructure.
Trusted Platform Module (TPM) Specification 1.2, revision 94, 29 March 2006, Unclassified	Summary: The Trusted Computing Platform Alliance (TCPA) main specification is an industry specification that enables trust in computing platforms in general.
IETF RFC 5792, PA-TNC A Posture Attribute Protocol Compatible with TNC, March 2010, Unclassified	Summary: This document specifies Posture Attribute-TNC (PA-TNC), a Posture Attribute Protocol identical to the Trusted Computing Group's IF-M 1.0 protocol and evaluates PA-TNC against the requirements defined in the Network Endpoint Assessment (NEA) Requirements specification.
IETF RFC 5793, PB-TNC A Posture Broker Protocol Compatible with TNC, March 2010, Unclassified	Summary: This document specifies Posture Broker-TNC (PB-TNC), a Posture Broker Protocol identical to the Trusted Computing Group's IF-TNCCS 2.0 protocol and evaluates PB-TNC against the requirements defined in the NEA Requirements specification.
IETF RFC 2753, A Framework for Policy-Based Admission Control, January 2000, Unclassified	Summary: This document specifies a framework for providing policy-based control over admission control decisions. In particular, it focuses on policy-based control over admission control using Resource Reservation Protocol (RSVP) as an example of the quality of service (QoS) signaling mechanism.
ISO/IEC 8348:2002, Open Systems Interconnection – Network service definition, 20 March 2008, Unclassified	Summary: This document specifies Open System Interconnection (OSI) network layer protocols and services and describes other OSI network layer specifications.

10 Cost Considerations

This section provides examples of some of the types of costs that the Organization will need to consider when implementing this Capability. The following examples are costs that are common across all of the Community Gold Standards Capabilities:

1. Solution used for implementation (hardware and/or software)
2. Necessary training
3. Licensing (if applicable)
4. Lifecycle maintenance
5. Impact/dependency on existing services
6. Manpower to implement, maintain, and execute
7. Time to implement, maintain, and execute
8. Network bandwidth availability and consumption
9. Scalability of the solution relative to the Enterprise
10. Storage and processing requirements

In addition to the common costs, the following are examples of cost considerations that are specific to this Capability:

1. Solution used for implementation–The solution(s) will need to be scalable to fulfill the Enterprise needs as it grows.
2. Scope of work–Each enforcement point will require resources to operate. The greater the number of enforcement points, the greater the total cost of operation.

11 Guidance Statements

This section provides Guidance Statements, which have been extracted from Section 3 (Capability Gold Standard Guidance) of this Capability document. The Guidance Statements are intended to provide an Organization with a list of standalone statements that are representative of the narrative guidance provided in Section 3. Below are the Guidance Statements for the Network Access Control Capability.

- The Enterprise shall provide a set of policies and procedures that is used to manage access to a network and all of its associated systems or resources including both connections coming into the Enterprise from external networks and connections traversing enclave boundaries internal to the Enterprise.
- The network access control system shall perform platform authentication for all hosts on the network.
- The network access control system shall prevent the attachment of rogue devices on the network, including access points and wireless devices.

- Devices and systems shall be reauthenticated as needed by the network access control system to prevent changes in the identity of previously authorized devices connected to the network.
- Network access control shall use hardware modules (e.g., TPM) on the connecting device for storage of the authentication attributes, which shall be cryptographically protected.
- Cryptographic modules shall be compliant with any applicable federal and Community standards.
- The network access control system shall use attributes that have been authenticated to make an access decision before providing network services to platforms.
- There shall be an enforcement point at network boundaries that can effectively block access to resources in accordance with defined access policy.
- The association between the attributes and the identity shall be ensured, such as by using cryptographic binding, thus making the identity and attributes suitable for use by the enforcement point to make the access decisions.
- Network access control shall ensure the platform complies with network access policy, including the functions of verifying the presence, status, and software version of mandated applications (including the operating system); completeness of virus signature databases; completeness of intrusion detection and prevention systems; and the acceptable patch level of all software.
- Network access control policies shall extend to virtualized systems, including both the guest virtual machine and the host system running the virtualization software.
- To enable assessment by the network access control system, endpoints shall support the Platform Trust Services Interface Specification that supports the collection of endpoint integrity status and detection of unauthorized modification. The endpoint shall store integrity information in the protected hardware module.
- Endpoints shall be isolated until the completion of their assessment by the network access control system.
- When the network access control system completes its assessment of an endpoint, that endpoint shall be granted full access, limited access, or remain isolated, as appropriate.
- Isolation, limited access, remediation, and operational networks shall exist to allow for secure segregation in a network access control system.
- Technology measures shall be in place to enforce isolation of unauthenticated or platforms not in compliance with access policies.

- While a platform is isolated because of non-compliance with access policies, actions shall be taken to ascertain the issues with the endpoint's integrity, and the necessary steps to alleviate these issues shall be taken, if possible.
- Platforms shall be reassessed prior to being granted network access after implementing the necessary remediation steps to become compliant with access policies.
- All actions taken by the network access control system shall be stored as auditable events and audited in accordance with Enterprise policy.
- The network access control system shall provide reports and alerts to network enterprise monitoring systems for trend analysis and situational awareness of network activity.